MAKING THE APEC CROSS-BORDER PRIVACY RULES SCALABLE

Report from Manila, Philippines APEC CBPR Workshop, December 5-6, 2018

SUMMARY

There is widespread interest in expanding micro, small and medium-sized enterprise (MSME) participation in the APEC Cross-Border Privacy Rules (CBPR) System, but MSMEs face particular challenges navigating the web of country-specific privacy laws and regulations that apply to their organizations, understanding how CBPR certification can benefit them, and justifying the cost of certification. APEC, member economies and other stakeholders can help remove these barriers by working to promote awareness of the CBPR System including through increased economy participation, developing practical tools for interested organizations, increasing the number of APEC-recognized Accountability Agents (AAs), and facilitating interoperability between the CBPR System and other privacy regimes.

INTRODUCTION

The rapid global expansion of the Internet to more than 47% of the global population[1] has fueled economic growth and enabled innovation across all sectors of the economy, contributing as much as $2.8 trillion in impact on the global economy[2]. Yet alongside growth, concerns have emerged about consumer privacy as personal information crosses international borders. Governments have responded by adopting laws, regulations and policies to address these concerns.

The differences between these policies have created obstacles for companies that must transfer data between countries with disparate data protection regimes. In 2011, the leaders of the 21 APEC economies endorsed the CBPR System, which is designed to bridge these differences and facilitate data flows within the Asia-Pacific region. The CBPR System is based on the APEC Privacy Framework, which lays out nine high-level principles for protecting consumers' personal information. Accountability Agents, APEC-recognized entities, certify organizations' compliance with the high privacy and data security standards embodied in the CBPR program requirements.[3] APEC has also developed a complementary system called Privacy Recognition for Processors (PRP), which enables organizations processing personal information to demonstrate their compliance with the PRP program requirements to APEC-certified AAs.

The United States, Japan, Mexico, Canada, Singapore and the Republic of Korea currently participate in the CBPR System. Australia, Chinese Taipei and the Republic of the Philippines are in the process of joining. The United States was the first economy to join the PRP System in

[1] "The State of Broadband." Sept 2016. United Nations Broadband Commission, available at http://www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf

[2] "Digital globalization: The new era of global flows." Feb 2016. McKinsey Global Institute.

[3] For those interested in learning more about the benefits of the CBPR System for governments and companies, see the 2016 report "Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR System," available at http://unctad.org/meetings/fr/Contribution/dtl_eweek2016_IIS-APEC_en.pdf.

2017, followed quickly by Singapore in early 2018. As of the time this report was written, 23 companies had obtained CBPR certifications from the two APEC-recognized Accountability Agents: TRUSTe and JIPDEC.

Thus far, almost all the companies that have obtained CBPR certification are large multinational corporations.[4] APEC economies have expressed their interest in making certifications more accessible and beneficial to companies of all sizes, and particularly to MSMEs. In Manila, Philippines in December 2017, the U.S. Department of Commerce and the Philippine National Privacy Commission brought together experts and stakeholders from industry, governments, and trade associations in the CBPR System at a workshop (hereafter referred to as the "Manila workshop") to identify the barriers to MSME participation in the CBPR System and make recommendations to APEC, governments, and AAs.

CHALLENGES TO CBPR PARTICIPATION BY MSMEs

The challenges identified at the Manila workshop can be grouped into three broad categories: lack of awareness of the CBPR System, confusion over the proliferation of privacy regimes and certifications, and difficulty justifying the perceived cost and administrative work of obtaining CBPR certification.

1. Lack of Awareness

Because MSMEs often lack large numbers of dedicated legal and compliance staff to ensure compliance with the latest developments in privacy and data protection internationally, perhaps the top barrier to participation in the CBPR System is a lack of awareness. Often MSMEs are unaware of the System's existence, and even those that have heard of it are unfamiliar with the basics of how it works, the benefits of participation and the process of obtaining a certification. Further, Participants expressed concern that existing publications about the CBPR System are lengthy and complex for non-technical experts.

2. Confusion about legal and regulatory regimes

Many companies expressed confusion about the proliferation of privacy and data protection laws that apply to their companies. MSMEs claimed that they find it difficult to understand which rules and regulations apply to their organizations, how to reconcile conflicts between them, and which certifications will be the most beneficial based on their organization's situation. Companies in the Philippines, for example, are already focused on compliance with the Philippines Data Privacy Act and, depending on their main export markets, new data protection regimes in the European Union, Japan, Singapore and other trade partners. With limited resources, many MSMEs feel that they do not have sufficient time to evaluate, become compliant with, and apply for APEC CBPR certification, even though companies noted that many compliance requirements under the CBPR System, Japan's Act on the Protection of Personal

[4] A list of certified companies is available on the homepage of http://cbprs.org/ under "Compliance Directory."

Information (APPI) and the European Union General Data Protection Regulation (GDPR), among others, are substantially similar.

In countries where multiple privacy certifications exist, some companies have expressed confusion over the differences between them and have found it difficult to make the business case to pay fees for multiple certifications. In Japan, for example, companies who meet certain privacy standards have been able to obtain the PrivacyMark (known as the "P-Mark") certification from JIPDEC since 1998, and in the United States, thousands of companies have self-certified to the EU-U.S. Privacy Shield Framework, which helps to facilitate compliance with the European Union's privacy standards for transferring data to the United States.

3. Administrative burden and financial costs

In addition to the cost of applying for a CBPR certification, companies must also consider the ongoing administrative and financial resources that will be necessary to maintain CBPR-compliant practices. With limited financial and staffing resources, MSMEs claimed they often prioritize product development and marketing, while attempting to limit overhead costs, including legal and compliance costs. Private sector participants at the Manila workshop expressed that they have had difficulty convincing the leadership of their organizations that attaining and maintaining CBPR certification should be prioritized over other needs.

STRATEGIES AND BEST PRACTICES

Over the course of the workshop, participants highlighted several strategies and best practices that APEC, member economies, and other stakeholders can implement to address the barriers discussed above. As set forth below, the APEC Electronic Commerce Steering Group (ECSG) and the Data Privacy Subgroup (DPS), which developed and oversee the CBPR System, can coordinate much of the work needed to make CBPR certification more accessible to and beneficial for MSMEs. There are also important roles for the APEC Secretariat, economies, AAs and industry stakeholders to play.

1. Improve public communications

In 2017, the ECSG and DPS recognized the importance of improving public communications about the CBPR System by adopting a strategic plan for communications, prioritizing an overhaul of the public-facing website (cbprs.org) and communications documents to improve outreach. The enhanced website can be used as the central public portal for APEC- and economy-developed promotional materials and information about the CBPR System and its benefits for all stakeholders.

Participants emphasized that communications should be succinct and clear to general audiences, and suggested publishing one-page fliers, infographics, and booklets in non-technical language. In addition, participants highlighted that all stakeholders – including governments (trade, regulatory, and enforcement authorities), trade associations, think tanks, AAs and participating

companies[5]--have an important role to play in raising awareness of the CBPR System and can use the enhanced communications tools to further disseminate information about the system.

2. Develop practical tools for companies

AAs have noted that the cost of obtaining a CBPR certification partly depends on the extent to which companies have already aligned their policies and practices with the CBPR requirements and other international data protection standards before applying for certification. The more a company's policies and practices reflect the CBPR program requirements, the less time the AA must spend consulting with the company during the certification process. To reduce the cost of CBPR certification, APEC can take steps to help companies prepare for the certification process. Such steps may include developing enhanced checklists and other tools for companies, and facilitating educational webinars and workshops, and mapping how the CBPR certification requirements align with other privacy and data protection practices and requirements. These efforts could be geared toward companies of varying sizes and in a range of industries. Trade associations, think tanks and NGOs can also play a role in educating MSMEs about how to implement strong privacy policies and practices, and how to apply for CBPR certification to reduce costs for MSMEs.

3. Offer concrete benefits to participating companies

Economies should consider offering concrete benefits to companies that have undertaken the effort to comply with CBPR requirements, including, where appropriate, allowing organizations to fulfil domestic legal requirements through CBPR certification, or mitigating enforcement penalties for CBPR-certified companies. For example, Japan's data protection authority, the Personal Information Protection Commission, has recognized CBPR certification as a valid mechanism for transferring personal information out of Japan. As such, CBPR-certified organizations may transfer information from Japan to another economy. Similarly, the Republic of Korea has stated it is considering offering reduced fines for CBPR-certified companies that experience data breaches and data privacy law violations. The U.S. Federal Trade Commission previously has stated that to the extent strong privacy codes of conduct are developed, it would view adherence to such codes favorably in connection with its law enforcement work. Concrete benefits such as these may make it easier for MSMEs to justify the cost of applying for and maintaining CBPR certification.

4. Explore the full range of AA models

[5] For example, at the time of the Manila workshop, Japan's Privacy Enforcement Authority, the Personal Information Protection Commission, had held 90 CBPR seminars attended by over 13,000 people. It has also presented on the CBPR System at conferences including the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and Asia Pacific Privacy Authorities (APPA) Forum.

The CBPR System provides AAs with the flexibility to develop different business models to serve clients of various sizes and needs. AAs can be private, public or non-profit entities, and there is no APEC-imposed limit on how many AAs can work in each economy. AAs may offer certifications across multiple jurisdictions if they meet domestic legal requirements. However, no more than one AA currently operates in any participating economy.

As a first step toward expanding the number of AAs offering certifications to companies, APEC could commission a report describing the range of potential business models that would fulfil the baseline requirements for AAs. For example, the report could explore how Accountability Agents might operate using the accounting/audit model, or how AAs might outsource components of AA responsibilities, such as dispute resolution, to third parties.

5. Develop tools for AAs and engage in AA capacity-building

The two Accountability Agents currently recognized by APEC have substantial experience offering privacy-related certifications, but some economies lack entities with similar experience. APEC can help to fill this gap by facilitating the development of tools for AAs, including publishing practical information on the process of establishing an AA, selecting an AA business model, and applying for APEC recognition. Participating economies could also facilitate efforts to recruit and establish AAs, including through cooperative outreach.

6. Build bridges to other privacy regimes (facilitate global compliance)

CBPR certification provides a useful tool that companies can use to facilitate compliance with privacy laws worldwide. Specifically, as part of the application process, AAs help companies develop a comprehensive privacy program that helps them to meet not only APEC requirements, but also many of the requirements of other privacy regimes, including the EU-U.S. Privacy Shield and EU Binding Corporate Rules (BCR). MSMEs would benefit greatly from more formal and informal linkages between these regimes and the CBPR System. APEC successfully took a step in this direction in 2014 by working with the European Union (EU) to publish a referential[6] that maps the requirements of CBPR certification to EU requirements for BCR certification. Companies have used the referential to identify similarities between the two privacy frameworks and thereby streamline the BCR application process.[7]

In 2017, APEC and the EU agreed to explore interoperability between the CBPR System as well as the EU's new General Data Privacy Regulation (GDPR).[8] One possibility would be to offer a common application and set of standards to meet both CBPR certification requirements and the certification requirements under Article 42 of the GDPR. Another would be to allow companies to meet their due diligence requirements under Article 28.1 of the GDPR through CBPR

[6] https://iapp.org/resources/article/referential-bcr-cbpr-requirements/
[7] http://www.trustarc.com/blog/2016/03/22/merck-successfully-concludes-first-apec-based-bcr-approval/
[8] https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union

certification. Beyond the EU, APEC could also consider expanding participation in the CBPR System to economies outside of APEC or explore mutual recognition with certifications in non-APEC economies.

7. Build links to domestic privacy certifications

APEC economies can also reduce compliance costs for MSMEs by building links between domestic privacy certifications and CBPR certification. At the Manila workshop, the Republic of Korea noted that it is developing a joint application for CBPR and PIMS, a domestic certification which indicates organizations' compliance with domestic privacy laws and regulations.[9] Singapore also indicated that it is exploring ways to develop a domestic privacy mark which is linked to CBPR and PRP certifications for cross-border transfers.

8. Expand access to the Privacy Recognition for Processors (PRP) System

Organizations that process information on behalf of others may find that PRP certification is more practical than CBPR certification. Since PRP has fewer requirements, certification would likely require less time and money, making it an attractive option for MSMEs. However, only the United States and Singapore have joined the PRP System so far, and no AAs currently offer PRP certifications. APEC can help to facilitate access to the PRP System by actively working to promote the benefits of the PRP System and to recruit AAs to offer PRP certification.

9. Establish an MSME Working Group in the APEC Data Privacy Subgroup

Many stakeholders recommended that the DPS establish a working group, composed of governments, PEAs, AAs and companies of various sizes, tasked with addressing the barriers identified at the workshop and implementing the recommendations outlined in this report. The working group could ensure that the ideas discussed at the workshop are explored in depth and adopted as appropriate, while also ensuring that all interested stakeholders have a voice in shaping how solutions are developed and executed.

[9] As of September 2017, 71 organizations in the Republic of Korea had received a PIMS certification.